Эссе по курсу «Защита информации»
на тему

«Обзор технологии EDGE: основные принципы обеспечения безопасности»

Шерстнёв А.Е.
Гр.112

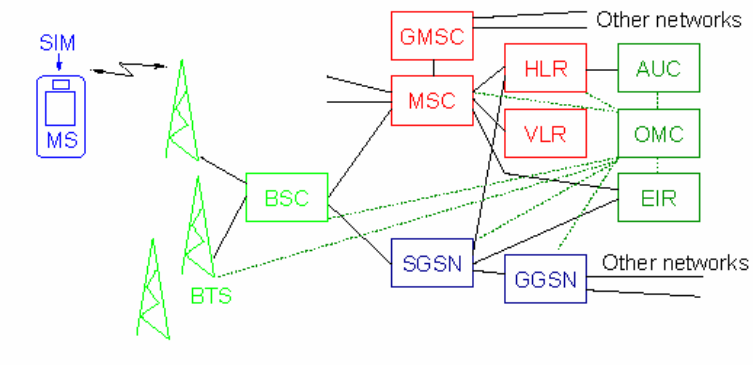
2005

Введение.

Стандарт EDGE, также известный как EGPRS, появился в 1999 году. Его разработка явилась одним из этапов перехода от систем второго поколения(GSM) к третьему(UMTS). Эта технология вносит ряд заметных улучшений в существующий стандарт(GPRS), без значительной переработки основных структурных узлов. EDGE использует прежнюю структуру множественного доступа с временным разделением(TDMA) – одновременно одну и ту же частоту могут использовать 8 абонентов(8 таймслотов/200кГц). Каждый таймслот представляет физический канал и может быть использован как для передачи пользовательских данных, так и для служебной информации (сигналов управления). Оператор обычно предоставляет несколько частотных диапазонов, поэтому GSM является комбинацией TDMA и FDMA(Frequency Division Multiple Access).

Важно понимать, что по своей сути EDGE является надстройкой над GPRS, используемой, в конечном счете, только лишь для увеличения пропускной способности радиоканала, путём применения новых кодировок и схем модуляции. В новой технологии используются прежние принципы работы и архитектура сети.

Приведу некоторые пояснения о назначении узлов в GSM сети:



MS(Mobile station) = ME(Mobile Equipment) + SIM. SIM служит для аутентификации пользователя прежде, чем он получит доступ к сети. Также SIM содержит алгоритмы генерации ключа(A8) и аутентификации(A3). Алгоритм GEA3 реализован в ME

BSC(Base Station Controller) – Контроллер базовой станции. Этот модуль содержит уровни RLC и MAC, наиболее сильно подвергшиеся изменениям. О них речь пойдёт ниже.

SGSN(Serving GPRS Support Node) – узел, предоставляющий точку входа GPRS(EDGE) сервиса. Он отвечает за пересылку пакетов между пользователем и сетью.

GGSN(Gateway GPRS Support Node) – обеспечивает доступ к внешним сетям(например, Интернет). Основная роль – доставка пакетов к текущему местоположению MS. Этот узел ведёт таблицу соответствия между MS и определённым SGSN.

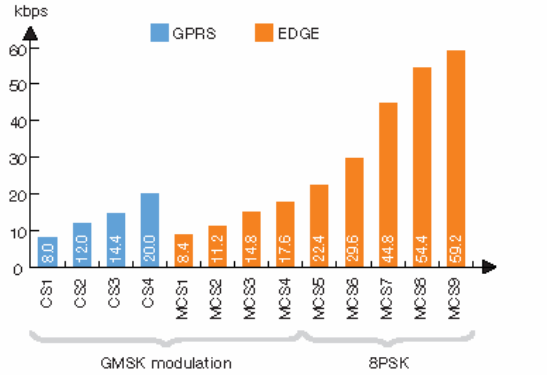
HLR(Home Location Register) – хранит данные о каждом пользователе.

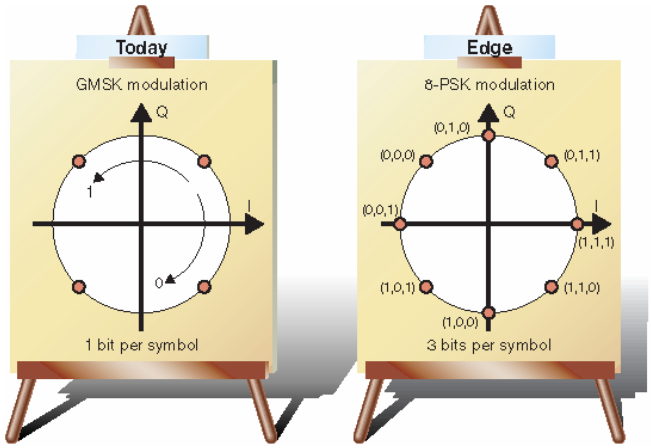
AuC(Authentication Center) – хранит аутентификационные данные пользователя

Единственное изменение в SGSN и GGSN, необходимое для перехода к EDGE – это увеличение скорости обмена данными. Поэтому, в дальнейшем, внимание будет сосредоточено в основном на уровнях узла BSC: PHY -> MAC -> RLC -> …

Физический уровень претерпел существенные изменения, т.к. в EDGE используется один из типов фазовой модуляции 8PSK(8-phase shift keying). В отличие от GMSK(Gaussian Minimum shift keying), применённой в GPRS, 8PSK при передаче одного символа позволяет передать 3 бита данных. Таким образом, при одинаковой скорости передачи символов, скорость передачи данных в EDGE в 3 раза выше. Так, если в GPRS максимально возможная скорость обмена была 172,8 кбит/с, то теперь теоретически достижимый предел равен 475 кбит/с. Обратной стороной такого подхода является более слабая помехозащищённость 8PSK(символы меньше отличаются друг от друга, чем в GMSK). Однако, при этом всегда остаётся возможность пользоваться модуляцией GMSK для совместимости оборудования или максимальной помехозащищённости в случае плохого качества связи.

В стандарте определено 9 схем кодирования сигнала:





При благоприятных условиях в радиоэфире недостатки 8PSK не играют существенной роли, но, тем не менее, наряду с полезной информацией предусмотрена передача дополнительных битов, служащих для детектирования и исправления возможных ошибок(incremental redundancy). Постепенное увеличение «избыточности» (от MCS9 до MCS1) обеспечивает максимальную пропускную способность канала при данных условиях передачи. Для восстановления данных, в дополнение к битам избыточности, используется информация, содержащаяся в ранее переданных блоках.

MAC(Medium Access Control).

На уровне MAC происходит распределение ресурсов между несколькими пользователями(MS). Также этот модуль контролирует очерёдность запросов и осуществляет разрешение конфликтов. Конфликты могут возникнуть как между несколькими MS при одновременном запросе доступа к одному ограниченному ресурсу, так и между несколькими сервисами одной станции.

Для передачи данных MAC может работать в одном из трёх режимов. Вот их краткое описание.

Динамическое распределение.

Данный подход позволяет использовать свободные каналы для передачи данных(PDCH), а в случае необходимости (например, поступил запрос от высокоприоритетного сервиса) эти каналы могут быть освобождены. Для координации использования канала используется флаг USF, который включается в заголовок каждого пакета. Этот флаг несёт информацию о том, какая MS сможет использовать данный PDCH для передачи данных в следующем таймслоте.
Т.к. USF может принимать 8 значений, один канал могут использовать 8 MS.

Расширенное динамическое распределение.

Отличается от предыдущего метода тем, что MS может пользоваться каналом на протяжении нескольких последующих таймслотов.

Фиксированное распределение.

Одна MS получает несколько каналов.

RLC(Radio Link Control)

Основные функции, выполняемые на уровне RLC: исправление ошибок, повторная передача, ресегментация.

Принцип ресегментации заключается в следующем: в GPRS перед началом посылки данных выбирается схема кодировки (в зависимости от состояния радиоэфира), далее блок данных разбивается на пакеты, которые отправляются последовательно. Если при передаче из-за усилившихся помех какие-то пакеты передались с ошибкой, для их повторной передачи использу-

ется та же кодировка. EDGE позволяет менять кодировку оперативно в зависимости от условий передачи, а при приёме "сшивать" пакеты с разной кодировкой. К тому же, в GPRS блок разбивается на 4 пакета, и при возникновении ошибки в одном из них приходится повторять передачу всех четырёх. В EDGE блок состоит из двух пакетов.

Важность выявления и исправления ошибок, произошедших при радиопередаче, на более низких уровнях состоит в том, что в случае прохождения в Интернет функция их отлавливания и исправления будет полностью возложена на протокол TCP. Очевидно, это займёт много времени и ресурсов. Для исправления ошибок RLC использует выборочную повторную передачу. При этом необходимо повторить передачу только части данных(frame), содержащую ошибку. Все правильно принятые фреймы буферизуются до тех пор, пока фрейм с ошибкой не ретранслируется, после чего они упорядочиваются и передаются на уровень выше(LLC - Logic Link Control). В функции RLC также входит сегментация фреймов LLC уровня для их последующей передачи по радиоканалу.

RLC обрабатывает 2 типа операций: с ответом(acnowledged) и без(unacknowledged). Как следует из названия, unacknowledged-операции не гарантируют доставку пакетов, но обладают постоянной задержкой их доставки. Такой режим используется при передаче в реальном времени непрерывного потока данных, например видео. При использовании acknowledged-операций работает механизм повторной передачи отдельных блоков, упомянутый выше.

Для сравнения, в GPRS перед отправкой информации RLC сначала делит её на порции по 128 блоков(пакетов) на 1 таймслот. Для каждого клиента устанавливается определённое число пакетов, которые могут быть отправлены последовательно до получения ответа(сообщения от приёмника о правильности принятых данных). Это число фиксировано и равно 64. Таким образом, пакеты, требующие ответа, располагаются в скользящем окне размером 64. Локальный адрес пакета на этой стадии - это его номер по модулю 64. Если окно начиналось на пакете с номером >64 и в промежутке от начала окна до 128-го пакета произошла ошибка, номер пакета, требующего повторной передачи, будет совпадать с номером «нового» пакета(расположенного в следующем таймслоте, т.е. с номером от 1 до 64). В таком случае необходимо заново передавать все данные предыдущего таймслота. Из этих соображений очевидно, что чем больше адресуемое число пакетов, тем меньше коллизий такого рода будет возникать.

В стандарте EDGE адресация пакетов расширена до 2048(конечно, бывает задействовано более 1 таймслота), а размер скользящего окна – до 1024. Такая техника, в конечном счете, также приводит к увеличению пропускной способности канала.

Т.к. защита на уровнях выше MAC не претерпела изменений по сравнению со стандартом GPRS, в этой работе будет рассмотрен низкоуровневый механизм выбора ключа, шифрования данных и сохранение их целостности. Далее в тексте встречается ещё несколько аббревиатур, используемых в стандарте GSM, но требующих пояснения:

SQN_{HE} – индивидуальная для каждого пользователя последовательность чисел(счётчик). Ведётся в HLR/AuC.

USIM(User Services Identity Module) – объединение узлов, выполняющих аутентификацию пользователя и генерацию ключа(на стороне MS).

IMEI(International Mobile Equipment Identity) – международный идентификатор аппаратуры, например, мобильного телефона. Жёстко «привязывается» к устройству при изготовлении.

IMSI(International Mobile Subscriber Identity) – международный идентификатор абонента. Выдаётся оператором, предоставляющим услуги сотовой связи, находится в SIM-карте.

TMSI(Temporary Mobile Subscriber Identity) – временный идентификатор абонента, может быть сгенерирован на месте текущего пребывания пользователя.

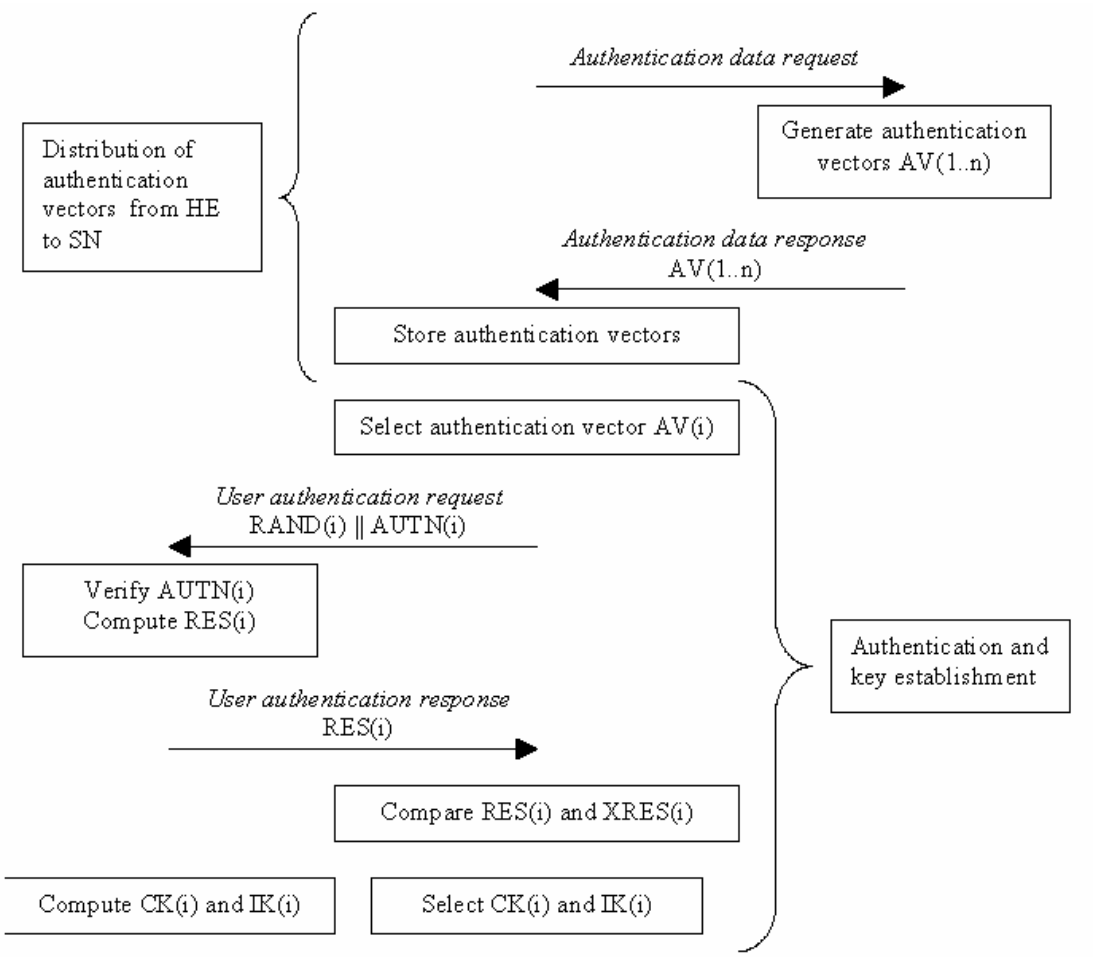
Перед началом коммуникационной сессии MS информирует сеть о своём присутствии, при этом SGSN прежде всего идентифицирует пользователя(по IMEI и/или IMSI/TMSI). В основном, эта процедура одинакова для всех GSM сервисов и служит для определения ключа K, который будет использоваться в дальнейшем для выполнения двусторонней аутентификации и выбора сессионного ключа в функциях алгоритмов A3 и A8(см. схемы). Оператор ассоциирует

K с конкретным IMSI при подключении пользователя, а при поступлении запроса от SGSN на основе этого ключа HE генерирует массив векторов AV[1..n] для аутентификации пользователя.

Рассмотрим механизм обмена ключами между USIM и SGSN. Синхронизация SGSN и USIM обеспечивается с помощью счётчика SQN_{HE} (на MS и HE) и числа SQN_{MS}. SQN_{HE} – это индивидуальный для каждого пользователя счётчик, SQN_{MS} – максимальное число в последовательности SQN_{HE}, принимаемое USIM**.**

Как уже упоминалось ранее, разработчики описываемого стандарта пытались достичь максимальной совместимости с существующей архитектурой GSM сетей, поэтому для передачи ключа используется уже известный протокол «запрос/ответ»(challenge/response).

Нужно отметить, что нижеописанная процедура происходит в предположении доверия пользователя HE и безопасности передачи данных между HE и SGSN.

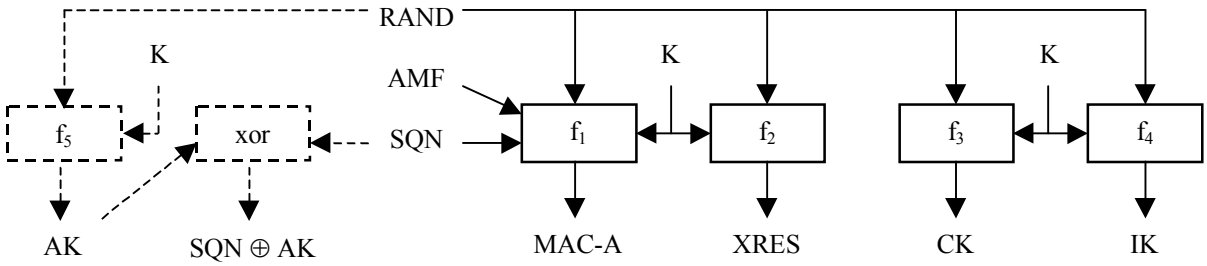


В общих чертах схема выглядит следующим образом: при получении запроса от SGSN, HE посылает в ответ последовательно массив n аутентификационных векторов(каждый из которых является аналогом «триплета» в GSM). Каждый вектор состоит из следующих частей: случайного числа RAND, ожидаемого ответа XRES, ключа CK, ключа целостности(integrity key) IK и аутентификационной метки AUTN. Каждый такой вектор годится для одной аутентификации и выбора ключа SGSN и USIM. Когда SGSN начинает процедуру определения ключа, выбирается следующий по порядку аутентификационный вектор и пользователю посылаются параметры RAND и AUTN (векторы организованы по принципу FIFO). Далее, USIM проверяет AUTN и, в случае принятия, генерирует ответ RES. При этом USIM вычисляет CK и IK. SGSN сравнивает принятый RES с XRES. При совпадении этих параметров процедуры аутентификации и обмена ключами считаются успешными. Вычисленные таким образом CK и IK передаются шифрующим модулям.

Чтобы сгенерированные описанным способом ключи не использовались неопределённо долго, в стандарте существуют механизмы их замены после передачи определённого объёма данных.(подробнее см.[1])

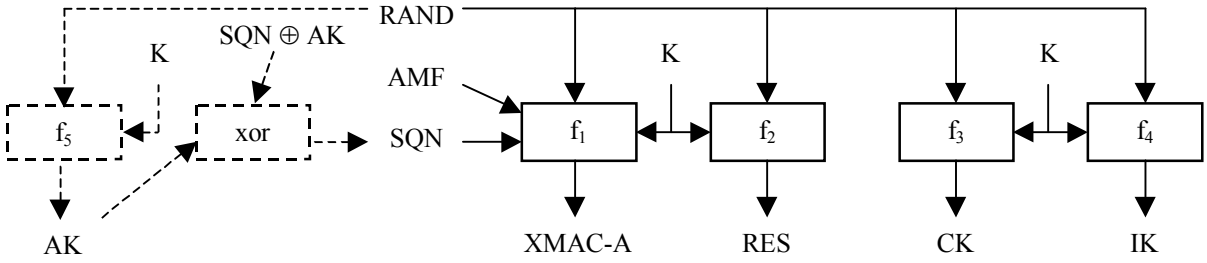
Для аутентификации, выбора ключа и шифрования данных используются алгоритмы A3, A8(основаны на блочном шифре Рэйндала(Rijndael)) и GEA3(модификация A5/3), разработанный Mitsubishi(кодовое имя MISTY),основан на блочном шифре Касуми(Kasumi), соответственно. Структура функций fi, а также схема GEA3 описаны в Приложении.

На нижеприведённых рисунках демонстрируется работа “клиентской” и “серверной” части процесса аутентификации.



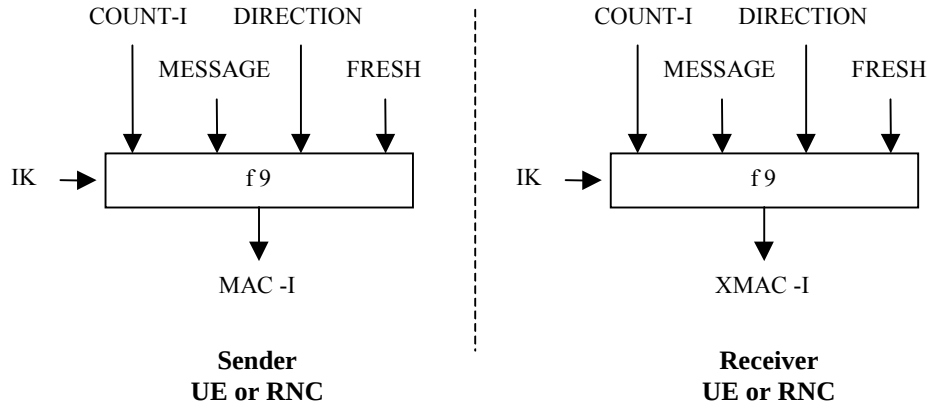
AUTN = SQN [⊕ AK] || AMF || MAC-A
Q = (RAND, XRES, CK, IK, AUTN)

Генерация аутентификационных векторов: По требованию SGSN HE определяет нужное количество векторов и извлекает их из базы данных HLR или же вычисляет новую последовательность(по ключу K). Далее массив векторов отсылается SGSN. В процессе работы HE контролирует индивидуальный счётчик SQN_{HE} каждого пользователя.



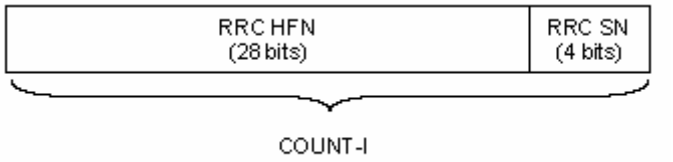
Определение ключа: Прежде всего, USIM восстанавливает ключ AK и последовательность SQN. Далее, вычисленный XMAC сравнивается с принятым MAC из AUTN. При несовпадении MS посылает SGSN отказ от аутентификации. SGSN в свою очередь генерирует отчёт об ошибке для HLR. В то же время SGSN может попытаться повторить процедуру. В этом случае дальнейшее поведение системы относится к процессу ресинхронизации, полное описание которого можно найти в A33102-620

Далее речь пойдёт о защите целостности данных(data integrity). Защита целостности реализована на уровне RRC(Radio Resource Control – следующий за RLC уровень). Для этого используется ключ IK.



Входными параметрами алгоритма являются: ключ целостности IK(integrity key), последовательность чисел COUNT-I, случайное число FRESH, сгенерированное на стороне сети, направление DIRECTION и сообщение MESSAGE. Основываясь на этих данных, пользователь вычисляет аутентификационный код сообщения(message authentication code) целостности данных MAC-I. Затем MAC-I применяется к отсылаемому сообщению. Получатель вычисляет XMAC-I полученного сообщения аналогичным образом и проверяет целостность данных путём сравнения XMAC-I с MAC-I.

COUNT-I [31:0]:



При отправке сообщения HFN(Hiperframe Number) инкрементируется. При этом пользователь хранит максимальное значение HFN от предыдущей коммуникационной сессии и при следующей установке связи сообщает обслуживающей сети начальное значение HFN. Этот принцип не позволяет использовать одинаковое значение счётчика с одним и тем же ключом.

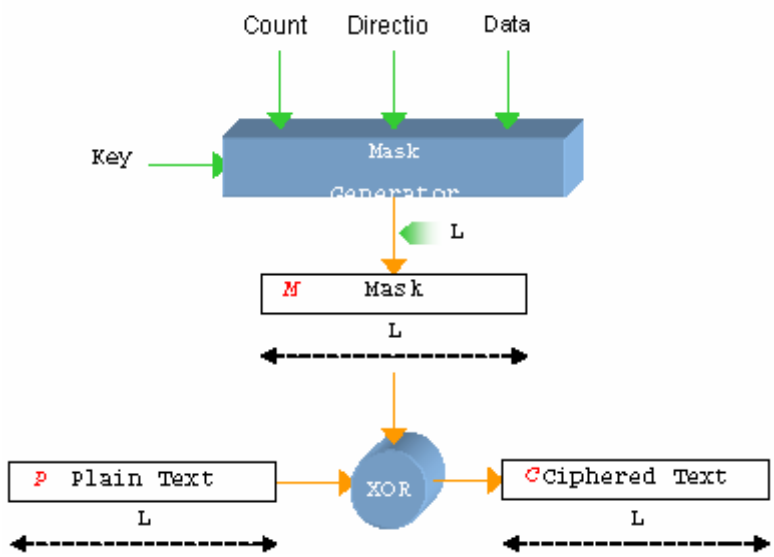
FRESH [31:0] – случайное число, генерируемое BSC. Этот параметр исключает использование пользователем “чужих” MAC-I в том случае, если одновременно установились соединения с одинаковыми IK.

MESSAGE – передаваемое сообщение.
DIRECTION – бит, индицирующий направление передачи сообщения.
Размер MAC-I составляет 32 бита.

Теперь рассмотрим подробнее непосредственно шифрование данных в EDGE. Замечу, что при разработке метода шифрования преследовались следующие цели:

- Неявная синхронизация процесса шифрования, включающая случаи передачи управления(Implicit synchronization of ciphering including handover cases)
- Одинаковый подход к сервисам реального времени и остальным
- «Увеличивающаяся избыточность»
- Использование существующих принципов и схем
- Мультиплицирование нескольких пользователей в 1 таймслот

Основной принцип описывается следующей схемой:



Шифрованные данные получаются по формуле: $C = M \oplus P$

Наиболее важным параметром для генерации маски является ключ. Остальные используются для различных процессов шифрования (создания масок) блоков в одном или нескольких потоках данных, в основном для исключения ситуации, когда с помощью одинаковых масок шифруются различные блоки данных. Очевидно, применение таких масок к блокам, которые будут в дальнейшем связаны, ведёт к существенной потере секретности:

$$\begin{array}{l} P_1 \oplus M = C_1 \\ \oplus \quad P_2 \oplus M = C_2 \\ \hline P_1 \oplus P_2 = C_1 \oplus C_2 \end{array}$$

L(Length) – длина шифруемого сообщения(16 бит) в битах, может принимать значение от 24 до 5000.
Data – идентификатор канала передачи данных (Bearer).
Остальные параметры аналогичны описанным при рассмотрении целостности.

Процесс шифрования проходит на одном из уровней: MAC (открытый(transparent) режим) или RLC (закрытый(non-transparent) режим). Не углубляясь в подробности, замечу только, что открытый режим используется обычно для передачи голоса, а закрытый – для передачи данных.

Несколько слов о безопасности сетей GSM 2.5G (к которым относится EDGE). Для совместимости с существующим стандартом алгоритмы аутентификации (A3) и выбора ключа (A8) остались без изменений.

Что касается защищённости передаваемых данных (в частности, алгоритма GEA3), явным образом сравнить сами алгоритмы A5/1, A5/2, используемые в сетях второго поколения (GSM 2G) с GEA3 (A5/3), в данной работе не представляется возможным, т.к. официально спецификации алгоритмов A5/1, A5/2 в силу малопонятных причин до сих пор закрыты. Но неоспоримым фактом является их взлом. Приведу два основных типа атак на GSM 2G:

1. Расшифровка переданных сообщений без знания ключа (атака на сам алгоритм).

   Не буду сильно углубляться в теорию этой проблемы, т.к. заинтересовавшимся не составит труда найти исчерпывающую информацию по данному вопросу в любом поисковике. Замечу лишь, что наиболее слабый алгоритм взламывается на обычном компьютере за время, меньшее 1 секунды (однако, подготовка требует нескольких часов вычислений). К примеру, слабым местом A5/2 было то, что шифрование производилось после внесения избыточности(для исправления ошибок при приёме) в данные. Как оказалось, такое искусствен-

ное «увеличение информации» сильно помогает при дешифровке.

2. Посредник между телефоном и базовой станцией (атака на процедуру аутентификации).

Т.к. в GSM 2G происходит односторонняя аутентификация: базовая станция авторизует телефон, но не наоборот, злоумышленник может выступать в качестве посредника между пользователем и базовой станцией. Далее, действия следующие: начинаем коммуникационную сессию с пользователем от имени базовой станции, сообщаем ему об использовании алгоритма A5/2(т.к. его проще всего взломать) и определяем секретный ключ K, о котором речь шла выше. Теперь хакер способен практически в полной мере дешифровать более сложные для анализа A5/1,3 во время обмена данными между пользователем и настоящей базовой станцией.

Как было показано выше, в системах 2.5G аутентифицируется как пользователь(сравнение RES с XRES), так и базовая станция(MAC-A из AUTN ?= XMAC-A, вычисленный мобильным телефоном). К тому же, A5/3, как будто бы, лишён найденных недостатков, и, по заверениям разработчиков, на данный момент обеспечивает защищённость близкую к 100%.

В принципе, в настоящее время этого оказывается достаточно, хотя бы потому, что вскоре появятся системы 3-го поколения, где, как хочется надеяться, роль безопасности будет не последней и учтутся слабые места нынешних протоколов.

Заключение.

Несомненно, главным достоинством EDGE является значительное увеличение скорости передачи и улучшение качества связи без существенной доработки используемого оборудования. Имеется в виду, что узлы, входящие в ядро системы, такие как SGSN,GGSN,… не затрагиваются (т.к., их структура мало зависит от скорости передачи).

Несмотря на увеличение объёма передаваемых данных, возникающее при использовании подобного подхода, средняя скорость передачи информации увеличивается из-за сокращения повторных передач. Т.е. EDGE может в некоторой мере удовлетворить требования пользователей до полной стандартизации и отладки 3G систем.

Приложение.

Размерность основных параметров описанных алгоритмов:

Аутентификационный ключ:	[K] = 128 бит
Случайное число:	[RAND] = 128 бит
Последовательность чисел:	[SQN] = 48 бит
Код аутентификационного сообщения:	[MAC] = 64 бита
Ключи шифрования и целостности:	[CK] = [IK] = 128 бит
У аутентификационного ответа длина переменная:	[RES] = 4-16 байт

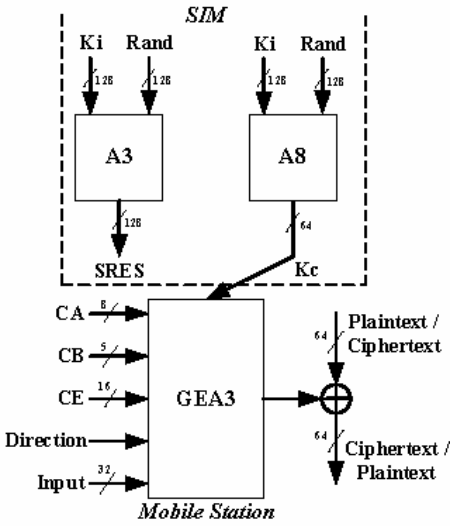


Figure 1. The GPRS security block diagram

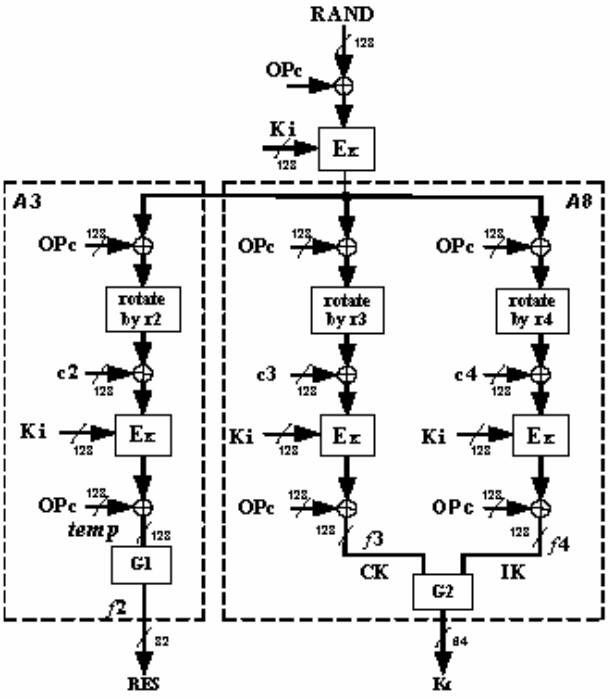


Figure 2. The A3 and A8 architectures

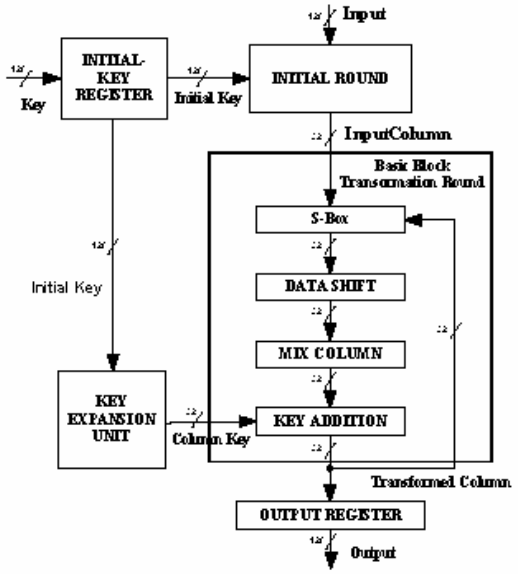


Figure 4. The RIJNDAEL block cipher implementation

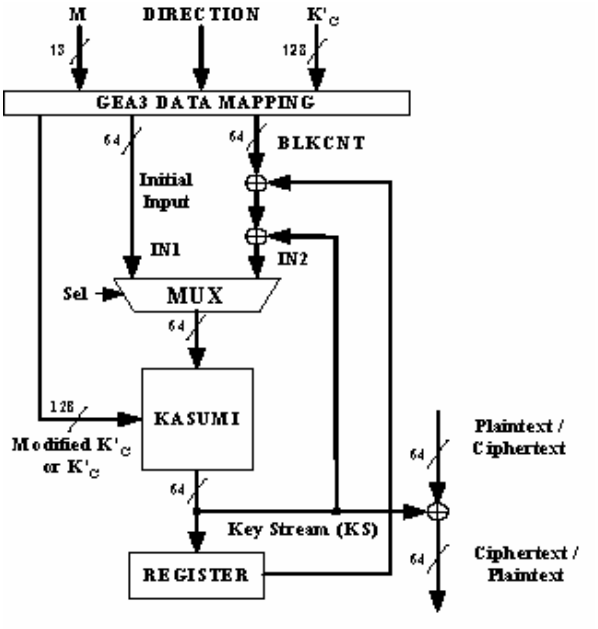


Figure 3. The GEA3 algorithm implementation

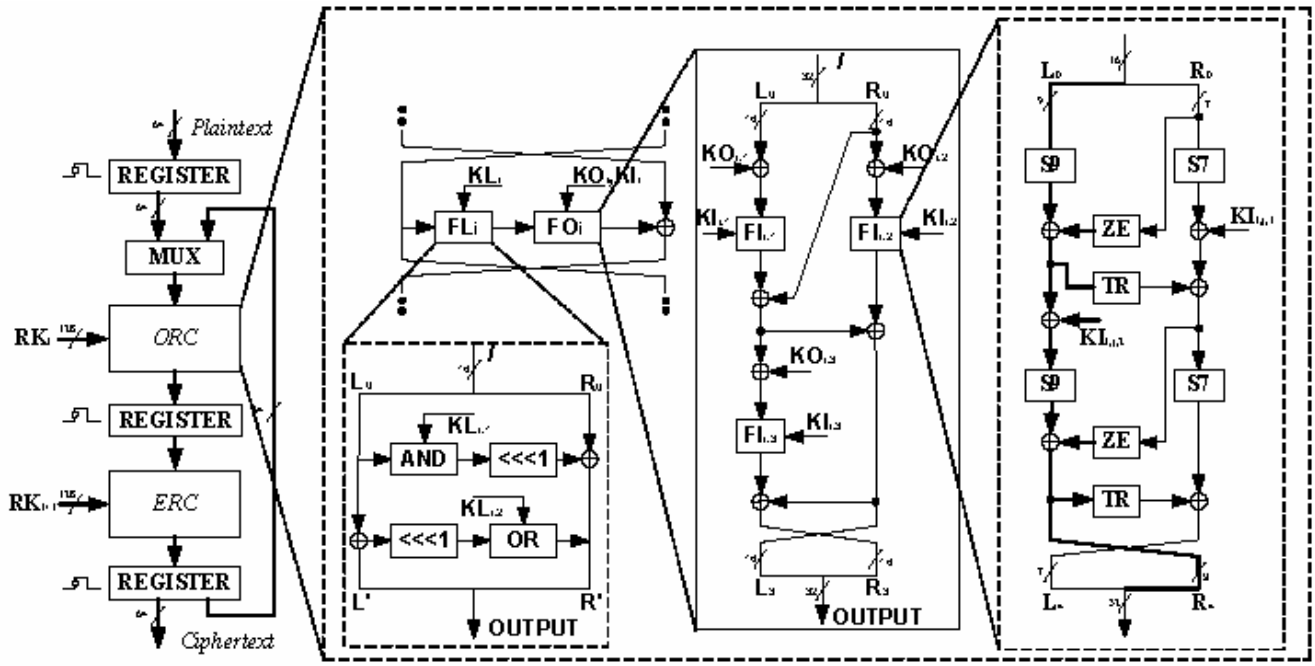


Figure 5. The KASUMI block cipher implementation

Использованная литература.

1. 3GPP TS 33.102 V6.2.0 (2004-09) “3G Security; Security architecture(Release 6)” www.arib.or.jp/IMT-2000/V430Dec04/ 2_T63/ARIB-STD-T63/Rel6/33/A33102-620.pdf
2. Deana Clover. “EGPRS (EDGE) - Enhancing the GSM GPRS System” engr.smu.edu/~jseraj/2003_termpapers/ Deana%20Branton%20EETS8316-EDGE-TermPaper.doc
3. ERICSSON Whitepaper. “EDGE. Introduction of high-speed data in GSM/GPRS networks”. www.ericsson.com/products/ white_papers_pdf/edge_wp_technical.pdf
4. P. Kitsos, N. Sklavos and O. Koufopavlou. “An End-to-End Hardware Approach Security for the GPRS” www.vlsi.ee.upatras.gr/~sklavos/ Papers/Papers04/Melecon04_GPRS.pdf
5. 3GPP TS 43.051 V5.9.0 (2003-04). “GSM/EDGE Radio Access Network; Overall description - Stage 2;(Release 5)” www7.informatik.uni-erlangen.de/~dulz/moko/2003/43051-590.pdf
6. Anders Furusk.r, Jonas N.slund and H.kan Olofsson. “Edge—Enhanced data rates for GSM and TDMA/136 evolution” stewks.ece.stevens-tech.edu/EE683/TechArticles/Ericsson/1999014.pdf
7. S3-000455 Nokia. “Ciphering parameters in GERAN” www.3gpp.org/ftp/tsg_sa/WG3_Security/ TSGS3_14_Oslo/Docs/PDF/S3-000455.pdf
8. 3GPP TS 33.105 V3.6.0 (2000-12). “3G Security; Cryptographic Algorithm Requirements(Release 1999)” 3gpp.org